Abstract

The invention allows the introduction in real-time of at least sufficient security to minimize the risk of intruders overhearing data on a particular link. This reduces the risk of being victim to either a Type 1 - Unauthorized access threat or a Type 3 - Message sequencing threat. The method involves encryption at the physical data link level where the form of the encryption affects groups of data bits. The effect of introducing the invention is to add noise to the signal in such a way that it can be subtracted from the received signal leaving only the original signal. The resulting signal, were it to be observed by a person other than the intended recipient, would have an effective Signal to Noise (S/N) ratio of less than 1. The masking effect of this added 'noise' signal hides the original signal from any eavesdroppers, since it well-known in the art that for a non-periodic signal to be effectively recovered it must have a S/N greater than 1.